PATENT
81942.0008
Express Mail Label No. EL 713 695 985 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Yasuyuki MURAKAMI

Serial No: Not assigned

Filed: January 23, 2001

For: SECRET KEY GENERATING METHOD, ENCRYPTION METHOD, CRYPTOGRAPHIC COMMUNICATION METHOD AND CRYPTOGRAPHIC COMMUNICATION SYSTEM

Art Unit: Not assigned

Examiner: Not assigned

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-016358 which was filed January 25, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: January 23, 2001

By: _____

Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:　２０００年　１月２５日

出願番号
Application Number:　特願２０００－０１６３５８

出願人
Applicant (s):　村田機械株式会社
笠原　正雄

２０００年　８月１８日

特許庁長官
Commissioner,
Patent Office　及川耕造

出証番号　出証特２０００－３０６４８４２

【書類名】　特許願
【整理番号】　20875
【提出日】　平成12年 1月25日
【あて先】　特許庁長官殿
【国際特許分類】　G09C 1/00
H04L 9/00
【発明の名称】　秘密鍵生成方法，暗号化方法及び暗号通信方法
【請求項の数】　3
【発明者】
【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内
【氏名】　村上　恭通
【特許出願人】
【識別番号】　000006297
【氏名又は名称】　村田機械株式会社
【代表者】　村田　純一
【特許出願人】
【識別番号】　597008636
【氏名又は名称】　笠原　正雄
【復代理人】
【識別番号】　100114557
【弁理士】
【氏名又は名称】　河野　英仁
【電話番号】　06-6944-4141
【代理人】
【識別番号】　100078868
【弁理士】
【氏名又は名称】　河野　登夫
【電話番号】　06-6944-4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　秘密鍵生成方法，暗号化方法及び暗号通信方法

【特許請求の範囲】

【請求項１】　複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする秘密鍵生成方法。

【請求項２】　複数のセンタの夫々にて、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティに対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする暗号化方法。

【請求項３】　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数のセンタ夫々は、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティに対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする暗号通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、センタにてエンティティ固有の秘密鍵を生成する秘密鍵生成方法、情報の内容が当事者以外にはわからないように情報を暗号化する暗号化方法、及び、暗号文にて通信を行う暗号通信方法に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化鍵と復号鍵とは、等しくても良いし、異なっていても良い。両者の鍵が等しい暗号系は、共通鍵暗号系と呼ばれ、米国商務省標準局が採用したＤＥＳ（Data Encryption Standards)はその典型例である。また、両者の鍵が異なる暗号

系の一例として、公開鍵暗号系と呼ばれる暗号系が提案された。この公開鍵暗号系は、暗号系を利用する各ユーザ（エンティティ）が暗号化鍵と復号鍵とを一対ずつ作成し、暗号化鍵を公開鍵リストにて公開し、復号鍵のみを秘密に保持するという暗号系である。公開鍵暗号系では、この一対となる暗号化鍵と復号鍵とが異なり、一方向性関数を利用することによって暗号化鍵から復号鍵を割り出せないという特徴を持たせている。

【０００５】

公開鍵暗号系は、暗号化鍵を公開するという画期的な暗号系であって、高度情報化社会の確立に必要な上述した３つの要素に適合するものであり、情報通信技術の分野等での利用を図るべく、その研究が活発に行われ、典型的な公開鍵暗号系としてＲＳＡ暗号系が提案された。このＲＳＡ暗号系は、一方向性関数として素因数分解の困難さを利用して実現されている。また、離散対数問題を解くことの困難さ（離散対数問題）を利用した公開鍵暗号系も種々の手法が提案されてきた。

【０００６】

また、各エンティティの住所，氏名等の個人を特定するＩＤ（Identity）情報を利用する暗号系が提案された。この暗号系では、ＩＤ情報に基づいて送受信者間で共通の暗号化鍵を生成する。また、このＩＤ情報に基づく暗号技法には、（１）暗号文通信に先立って送受信者間での予備通信を必要とする方式と、（２）暗号文通信に先立って送受信者間での予備通信を必要としない方式とがある。特に、（２）の手法は予備通信が不要であるので、エンティティの利便性が高く、将来の暗号系の中枢をなすものと考えられている。

【０００７】

この（２）の手法による暗号系は、ＩＤ－ＮＩＫＳ（ID-based non-interactive key sharing scheme)と呼ばれており、通信相手のＩＤ情報を用いて予備通信を行うことなく暗号化鍵を共有する方式を採用している。ＩＤ－ＮＩＫＳは、送受信者間で公開鍵，秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも必要としない方式であり、任意のエンティティ間で安全に通信を行える。

【０００８】

図５は、このＩＤ－ＮＩＫＳのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。図５において、エンティティＸの特定情報であるエンティティＸの名前，住所，電話番号等のＩＤ情報は、ハッシュ関数ｈ（・）を用いてｈ（ID_X）で表す。センタは任意のエンティティＸに対して、センタ公開情報｛PC_i｝，センタ秘密情報｛SC_i｝及びエンティティＸのＩＤ情報ｈ（ID_X）に基づいて、以下のように秘密情報S_{Xi}を計算し、秘密裏にエンティティＸへ配布する。

$$S_{Xi}=F_i\ (\{SC_i\},\ \{PC_i\},\ h(ID_X))$$

【０００９】

エンティティＸは他の任意のエンティティＹとの間で、暗号化，復号のための共通鍵K_{XY}を、エンティティＸ自身の秘密情報｛S_{Xi}｝，センタ公開情報｛PC_i｝及び相手先のエンティティＹのＩＤ情報ｈ（ID_Y）を用いて以下のように生成する。

$$K_{XY}=f\ (\{S_{Xi}\},\ \{PC_i\},\ h(ID_Y))$$

また、エンティティＹも同様にエンティティＸへの鍵を共通鍵K_{YX}を生成する。もし常に$K_{XY}=K_{YX}$の関係が成立すれば、この鍵K_{XY}，K_{YX}をエンティティＸ，Ｙ間で暗号化鍵，復号鍵として使用できる。

【００１０】

上述した公開鍵暗号系では、例えばＲＳＡ暗号系の場合にその公開鍵の長さは現在の電話番号の十数倍となり、極めて煩雑である。これに対して、ＩＤ－ＮＩＫＳでは、各ＩＤ情報を名簿という形式で登録しておけば、この名簿を参照して任意のエンティティとの間で共通鍵を生成することができる。従って、図５に示すようなＩＤ－ＮＩＫＳのシステムが安全に実現されれば、多数のエンティティが加入するコンピュータネットワーク上で便利な暗号系を構築できる。このような理由により、ＩＤ－ＮＩＫＳが将来の暗号系の中心になると期待されている。

【００１１】

このＩＤ－ＮＩＫＳには、次のような２つの問題点がある。一つは、センタがBig Brother となる（すべてのエンティティの秘密を握っており、Key Escrow S

ystem になってしまう）点である。もう一つは、ある数のエンティティが結託するとセンタの秘密を演算できる可能性がある点である。この結託問題については、これを計算量的に回避するための工夫が多数なされているが、完全な解決は困難である。

【００１２】

この結託問題の難しさは、特定情報（ＩＤ情報）に基づく秘密パラメータがセンタ秘密と個人秘密との二重構造になっていることに起因する。ＩＤ－ＮＩＫＳでは、センタの公開パラメータと個人の公開された特定情報（ＩＤ情報）とこの２種類の秘密パラメータとにて暗号系が構成され、しかも各エンティティが各自に配布された個人秘密を見せ合ってもセンタ秘密が露呈されないようにする必要がある。よって、その暗号系の構築の実現には解決すべき課題が多い。

【００１３】

そこで、本発明者等は、特定情報（ＩＤ情報）をいくつかに分割し、複数のセンタの夫々からその分割した特定情報（ＩＤ情報）に基づくすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えることができて、結託問題の回避を可能にし、その暗号系の構築が容易であるＩＤ－ＮＩＫＳによる秘密鍵生成方法，暗号化方法及び暗号通信方法（以下、これらを先行例という）を提案している。

【００１４】

結託問題を解決することを目的として提案されてきたエンティティの特定情報（ＩＤ情報）に基づく種々の暗号系が不成功となった理由は、エンティティの結託情報からセンタ秘密を割り出せないようにするための工夫を数学的構造に求め過ぎていたためである。数学的構造が複雑過ぎると、安全性を証明するための方法も困難となる。そこで、先行例の提案方法では、エンティティの特定情報（ＩＤ情報）をいくつかに分割し、分割した各特定情報（ＩＤ情報）についてすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えるようにする。

【００１５】

先行例では、信頼される複数のセンタが設けられ、各センタは各エンティティ

の分割した各特定情報（ＩＤ情報）に対応する数学的構造を持たない秘密鍵を夫々生成して、各エンティティへ送付する。各エンティティは、各センタから送られてきたこれらの秘密鍵と通信相手の公開されている特定情報（ＩＤ情報）とから共通鍵を、予備通信を行わずに生成する。よって、すべてのエンティティの秘密を１つのセンタが握るようなことはなく、各センタがBig Brother にならない。

【００１６】

【発明が解決しようとする課題】

そして、本発明者等は、このような先行例の改良を研究しており、その先行例を適用した暗号通信システムの構築を図っている。このような暗号通信システムにとっては、センタの数を増やすことにより安全性を向上することができる。従って、ある数のセンタにて実際に構築されている暗号通信システムに対して更なる新規のセンタを追加することが頻繁に行われると考えられる。

【００１７】

新規のセンタを暗号通信システムに追加参入させる度に、既存のセンタ及び新規のセンタに新しいハッシュ値を設定して全体の新しいハッシュ関数系を構築しなければならず、システム全体の変更が避けられない。システム全体を変更せずに、新規のセンタの追加に対応するためには、各センタが独自のハッシュ関数を公開する、予め十分に長いビット長のハッシュ関数を設定しておくなどの対策が考えられる。しかしながら、前者の対策では各エンティティが新たなハッシュ関数を鍵共有ソフトウェアに組み込むことが容易ではない、後者の対策ではいくら長いビット長のハッシュ関数を準備しておいてもセンタの追加数には限界があるという問題がある。

【００１８】

本発明は斯かる事情に鑑みてなされたものであり、新規のセンタを追加した場合においても既存のセンタのハッシュ値を変更する必要がなく、安全性を向上しながら多数の新規のセンタを容易に追加することができる秘密鍵生成方法，暗号化方法及び暗号通信方法を提供することを目的とする。

【００１９】

【課題を解決するための手段】

請求項１に係る秘密鍵生成方法は、複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする。

【００２０】

請求項２に係る暗号化方法は、複数のセンタの夫々にて、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティに対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする。

【００２１】

請求項３に係る暗号通信方法は、センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数のセンタ夫々は、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティに対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする。

【００２２】

本発明では、所定の複数ビット列からなる原ハッシュ値列から各センタ毎に複数の任意の順位のビットを選択して、選択した複数ビットを各センタ毎のハッシュ値として設定する。このようにすることにより、既存の各センタに複数ビットのハッシュ値が設定されていても、それらのハッシュ値を変更することなく、新規のセンタについて、原ハッシュ値列から選択した複数ビットにて、既存の各センタとは異なるハッシュ値を設定することができる。よって、既存の各センタのハッシュ値を変えることなく、多数の新規のセンタをＩＤ－ＮＩＫＳによる暗号通信システムに容易に追加することが可能となる。

【００２３】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（Ｊ個）のセンタ１が設定されており、これらのセンタ１としては、例えば社会の公的機関を該当できる。

【００２４】

これらの各センタ１と、この暗号通信システムを利用するユーザとしての複数の各エンティティａ，ｂ，…，ｚとは、通信路2_{a1}，…，2_{aJ}、2_{b1}，…，2_{bJ}、・・・、2_{z1}，…，2_{zJ}により接続されており、これらの通信路を介して各センタ１から各エンティティ固有の秘密鍵が各エンティティａ，ｂ，…，ｚへ伝送されるようになっている。また、２人のエンティティの間には通信路３ab，３az，３bz，…が設けられており、この通信路３ab，３az，３bz，…を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【００２５】

各エンティティの氏名，住所などを示す特定情報であるＩＤベクトルをＬ次元２進ベクトルとし、図２に示すようにそのＩＤベクトルをブロックサイズM_1，M_2，・・・，M_J毎にＪ個のブロックに分割する。例えば、エンティティｉのＩＤベクトル（ベクトルI_i）を下記（１）のように分割する。分割特定情報である各ベクトルI_{ij}（ｊ＝１，２，・・・，Ｊ）をＩＤ分割ベクトルと呼ぶ。ここで、M_j＝Ｍとすると、全てのＩＤ分割ベクトルのサイズが等しくなる。また

、M_j ＝１と設定することも可能である。なお、各エンティティの公開ＩＤベクトルはハッシュ関数により、Ｌビットに変換される。

【００２６】

【数１】

$$\overrightarrow{I_i} = [\overrightarrow{I_{i1}} | \overrightarrow{I_{i2}} | \cdots | \overrightarrow{I_{iJ}}] \quad \cdots (1)$$

【００２７】

（センタ１での準備処理）

センタ１は以下の公開鍵及び秘密鍵を準備し、公開鍵を公開する。

公開鍵　Ｐ　　大きな素数

Ｊ　　ＩＤベクトルの分割ブロック数

M_j　分割したＩＤベクトルのサイズ（ｊ＝１，２，・・・，Ｊ）

Ｌ　　ＩＤベクトルのサイズ（$L = M_1 + M_2 + \cdots + M_J$）

秘密鍵　ｇ　　ＧＦ（Ｐ）の原始元

H_j　乱数からなる$2^{Mj} \times 2^{Mj}$の対称行列

（ｊ＝１，２，・・・，Ｊ）

α_{ij}　エンティティｉの個人秘密乱数

（但し、$\alpha_{i1}\alpha_{i2}\cdots\alpha_{iK} \equiv 1 \pmod{P-1}$）

【００２８】

（エンティティの登録処理）

エンティティｉに登録を依頼された各センタ１は、準備した鍵とエンティティｉのＪ個のＩＤ分割ベクトルについて、それぞれに対応するＪ個の秘密鍵ベクトルs_{ij}（ｊ＝１，２，・・・，Ｊ）を以下の式（2-1），（2-2），・・・，（2-J）に従って求め、求めたベクトルs_{ij}を秘密裏に送って、登録を完了する。

【００２９】

【数２】

$$\overrightarrow{s_{i1}} \equiv g^{\alpha_{i1}H_1[\overrightarrow{I_{i1}}]} \pmod{P} \quad \cdots(2-1)$$

$$\overrightarrow{s_{i2}} \equiv \alpha_{i2}H_2[\overrightarrow{I_{i2}}] \pmod{P-1} \quad \cdots(2-2)$$

$$\vdots$$

$$\overrightarrow{s_{iJ}} \equiv \alpha_{iJ}H_J[\overrightarrow{I_{iJ}}] \pmod{P-1} \quad \cdots(2-J)$$

【００３０】

但し、ｇをスカラー、Ａ，Ｂを行列とした場合、$B = g^A$ はＡの各（μ，ν）成分についてｇのべき乗を行うことを表す。即ち、式（３）のようになる。また、H_j［ベクトルI_{ij}］は対称行列H_jからベクトルI_{ij}に対応した行を１行抜き出したものを表し、［・］の操作を参照と定義する。

【００３１】

【数３】

$$B_{\mu\nu} = g^{A\mu\nu} \quad \cdots(3)$$

【００３２】

（エンティティ間の共通鍵の生成処理）

エンティティｉは、自身の秘密鍵ベクトルs_{i1}の中から、エンティティｍのＩＤ分割ベクトルであるベクトルI_{m1}に対応する成分のベクトルs_{i1}［ベクトルI_{m1}］を選び出し、また、ｊ＝２，・・・，Ｊの各ブロックについて秘密鍵ベクトルs_{ij}の中から、ベクトルI_{mj}に対応する成分のベクトルs_{ij}［ベクトルI_{mj}］を各ブロック毎に選び出す。そして、Ｐを法とし、ベクトルs_{i1}［ベクトルI_{m1}］を底として残りのすべてのベクトルs_{ij}［ベクトルI_{mj}］（ｊ＝２，・・・，Ｊ）を順次べき乗することにより、共通鍵K_{im}を求める。このK_{im}を求める演算式は具体的に式（４）となり、このK_{im}はエンティティｍ側から求めた共通鍵K_{mi}と一致する。

【００３３】

【数４】

$$J_{im} \equiv \overrightarrow{s_{i1}}[\overrightarrow{I_{m1}}]^{\overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]\cdots\overrightarrow{s_{iJ}}[\overrightarrow{I_{mJ}}]}$$

$$\equiv g^{\alpha_{i1}\cdots\alpha_{iJ}} H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]\cdots H_J[\overrightarrow{I_{iJ}}][\overrightarrow{I_{mJ}}]$$

$$\equiv g^{H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]\cdots H_J[\overrightarrow{I_{iJ}}][\overrightarrow{I_{mJ}}]} \pmod P$$

・・・(４)

【００３４】

次に、上述した暗号システムにおけるエンティティ間の情報の通信について説明する。図３は、２人のエンティティａ，ｂ間における情報の通信状態を示す模式図である。図３の例は、エンティティａが平文（メッセージ）Ｍを暗号文Ｃに暗号化してそれをエンティティｂへ伝送し、エンティティｂがその暗号文Ｃを元の平文（メッセージ）Ｍに復号する場合を示している。

【００３５】

ｊ（ｊ＝１，２，・・・，Ｊ）番目のセンタ１には、各エンティティａ，ｂ固有のベクトルs_{aj}，s_{bj}（秘密鍵）を前記式（2-j)に従って求める秘密鍵生成器１ａが備えられている。そして、各エンティティａ，ｂから登録が依頼されると、そのエンティティａ，ｂの秘密鍵ベクトルs_{aj}，s_{bj}がエンティティａ，ｂへ送付される。

【００３６】

エンティティａ側には、Ｊ個の各センタ１から送られる固有の秘密鍵ベクトルs_{a1}，…，s_{aj}，…，s_{aJ}をテーブル形式で格納しているメモリ１０と、これらの秘密鍵ベクトルの中からエンティティｂに対応する成分であるベクトルs_{a1}［ベクトルI_{b1}］，…，ベクトルs_{aj}［ベクトルI_{bj}］，…，ベクトルs_{aJ}［ベクトルI_{bJ}］を選び出す成分選出器１１と、選び出されたこれらの成分を使用してエンティティａが求めるエンティティｂとの共通鍵K_{ab}を生成する共通鍵生成器１２と、共通鍵K_{ab}を用いて平文（メッセージ）Ｍを暗号文Ｃに暗号化して通信

路３０へ出力する暗号化器１３とが備えられている。

【００３７】

また、エンティティｂ側には、各センタ１から送られる固有の秘密鍵ベクトルs_{b1}，…，s_{bj}，…，s_{bJ}をテーブル形式で格納しているメモリ２０と、これらの秘密鍵ベクトルの中からエンティティａに対応する成分であるベクトルs_{b1}［ベクトルI_{a1}］，…，ベクトルs_{bj}［ベクトルI_{aj}］，…，ベクトルs_{bJ}［ベクトルI_{aJ}］を選び出す成分選出器２１と、選び出されたこれらの成分を使用してエンティティｂが求めるエンティティａとの共通鍵K_{ba}を生成する共通鍵生成器２２と、共通鍵K_{ba}を用いて通信路３０から入力した暗号文Ｃを平文（メッセージ）Ｍに復号して出力する復号器２３とが備えられている。

【００３８】

エンティティａからエンティティｂへ情報を伝送しようとする場合、まず、各センタ１で式（2-1），（2-2），…，（2-J)に従って求められて、予めメモリ１０に格納されている秘密鍵ベクトルs_{a1}，s_{a2}，…，s_{aJ}が成分選出器１１へ読み出される。そして、成分選出器11にて、エンティティｂに対応する成分であるベクトルs_{a1}［ベクトルI_{b1}］，ベクトルs_{a2}［ベクトルI_{b2}］，…，ベクトルs_{aJ}［ベクトルI_{bJ}］が選び出されて共通鍵生成器１２へ送られる。共通鍵生成器１２にて、これらの成分を使用して式（４）に従って共通鍵K_{ab}が求められ、暗号化器１３へ送られる。暗号化器１３において、この共通鍵K_{ab}を用いて平文（メッセージ）Ｍが暗号文Ｃに暗号化され、暗号文Ｃが通信路３０を介して伝送される。

【００３９】

通信路３０を伝送された暗号文Ｃはエンティティｂの復号器２３へ入力される。各センタ１で式（2-1），（2-2），…，（2-J)に従って求められて、予めメモリ２０に格納されている秘密鍵ベクトルs_{b1}，s_{b2}，…，s_{bJ}が成分選出器２１へ読み出される。そして、成分選出器２１にて、エンティティａに対応する成分であるベクトルs_{b1}［ベクトルI_{a1}］，ベクトルs_{b2}［ベクトルI_{a2}］，…，ベクトルs_{bJ}［ベクトルI_{aJ}］が選び出されて共通鍵生成器２２へ送られる。共通鍵生成器２２にて、これらの成分を使用して式（４）に従って共通鍵K_{ba}が求めら

れ、復号器２３へ送られる。復号器２３において、この共通鍵K_{ba}を用いて暗号文Ｃが平文（メッセージ）Ｍに復号される。

【００４０】

ここで、本発明の特徴部分である各センタ１でのハッシュ値の設定について説明する。以下の例では、図１に示したような暗号通信システムにおいて、４個（Ｊ＝４）のセンタ１が既存しており、これに新たに別の１または複数のセンタ１を追加する場合を考える。なお、各センタ１に設定するハッシュ値は１０ビットとする。

【００４１】

４個の新規のセンタ１を追加する場合に、各１０ビットずつの新しいハッシュ値を設定することになるが、従来では、全８個のセンタ１に対して８０ビットの新しいハッシュ関数系を構築するようにしている。よって、この場合には、既存のセンタ１のハッシュ値が変更されることになる。このように、従来では、新規のセンタを暗号通信システムに追加させる度に、ハッシュ値設定の面倒な処理を行わなければならない。

【００４２】

本発明では、次のようにして、追加した各センタ１の新しいハッシュ値を設定する。既存の４個の各センタ１におけるハッシュ値を並べたデータ列を所定の４０ビットの原ハッシュ値列（例えば、１番目のセンタ１でのハッシュ値が順位１～１０番目のビット、また、２番目，３番目，４番目のセンタ１でのハッシュ値が夫々順位１１～２０番目，２１～３０番目，３１～４０番目のビットとした構成）とし、新規の各センタ１毎に、その所定の４０ビットの原ハッシュ値列から既存の各センタ１での組合せと同じにならないように複数の任意の順位のビットを１０個選択して、選択した複数ビットをそのセンタ１のハッシュ値として設定する。例えば、この４０ビットの原ハッシュ値列から、１番目，３番目，８番目，１０番目，１６番目，２１番目，２２番目，２７番目，３３番目，３５番目のビットを選択してハッシュ値として設定する。このようなビットの選択パターンは$_{40}C_{10}$通りあり、非常に多数のセンタ１の追加に対応できる。

【００４３】

従って、本発明では、既存の４個の各センタ１におけるハッシュ値を変更することなく、新規追加の４個の各センタ１におけるハッシュ値を設定することができる。新規のセンタ１を追加した場合でも、ハッシュ関数系を設計し直す必要がない。よって、安全性を上げながら、極めて容易に多数の新規のセンタ１を追加することが可能である。

【００４４】

図４は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、各センタ１において各エンティティのＩＤベクトルとハッシュ値とを用いて各エンティティ固有の秘密鍵を生成する処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ４０は、各センタ１側に設けられている。

【００４５】

図４において、コンピュータ４０とオンライン接続する記録媒体４１は、コンピュータ４０の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体４１には前述の如きプログラム４１ａが記録されている。記録媒体４１から読み出されたプログラム４１ａがコンピュータ４０を制御することにより、各センタ１において各エンティティ固有の秘密鍵を生成する。

【００４６】

コンピュータ４０の内部に設けられた記録媒体４２は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体４２には前述の如きプログラム４２ａが記録されている。記録媒体４２から読み出されたプログラム４２ａがコンピュータ４０を制御することにより、各センタ１において各エンティティ固有の秘密鍵を生成する。

【００４７】

コンピュータ４０に設けられたディスクドライブ４０ａに装填して使用される記録媒体４３は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスクなどを用いてなり、記録媒体４３には前述の如きプログラム４３ａが記録されている。記録媒体４３から読み出されたプログラム４３ａがコンピ

ユータ４０を制御することにより、各センタ１において各エンティティ固有の秘密鍵を生成する。

【００４８】

【発明の効果】

以上詳述したように、本発明では、所定の複数ビット列から各センタ毎に複数の任意の順位のビットを選択することにより各センタ毎のハッシュ値を設定するようにしたので、既存のセンタのハッシュ値を変更することなく、新規のセンタについて、既存の各センタとは異なるハッシュ値を簡便に設定することができ、多数の新規のセンタをＩＤ－ＮＩＫＳによる暗号通信システムに容易に追加することが可能である。

【００４９】

（付記）

なお、以上の説明に対して更に以下の項を開示する。

（１）　送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を元の平文に復号する復号処理を、複数のエンティティ間で相互に行うこととし、各エンティティの特定情報を複数のブロックに分割した分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成して各エンティティへ送付する複数のセンタと、該センタから送付された自身の秘密鍵と通信対象のエンティティの特定情報に基づく公開鍵とを利用して前記暗号化処理及び復号処理に用いる共通鍵を生成する複数のエンティティとを有する暗号通信システムにおいて、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定するようにした暗号通信システム。

（２）　第（１）項の暗号通信システムであって、新規のセンタを既存の複数のセンタに追加した際に、前記既存の複数のセンタに設定されているハッシュ値を並べた原ハッシュ値列から任意の順位のものを選択することにより前記新規のセンタのハッシュ値を設定するようにした暗号通信システム。

（３）　コンピュータに、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、

前記エンティティ固有の秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、所定の複数ビット列から複数の任意の順位のものを選択することにより前記ハッシュ値を設定することをコンピュータに実行させるプログラムコード手段を含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図１】

本発明の暗号通信システムの構成を示す模式図である。

【図２】

エンティティのＩＤベクトルの分割例を示す模式図である。

【図３】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図４】

記録媒体の実施の形態の構成を示す図である。

【図５】

ＩＤ－ＮＩＫＳのシステムの原理構成図である。

【符号の説明】

１　センタ

１ａ　秘密鍵生成器

１０，２０　メモリ

１１，２１　成分選出器

１２，２２　共通鍵生成器

１３　暗号化器

２３　復号器

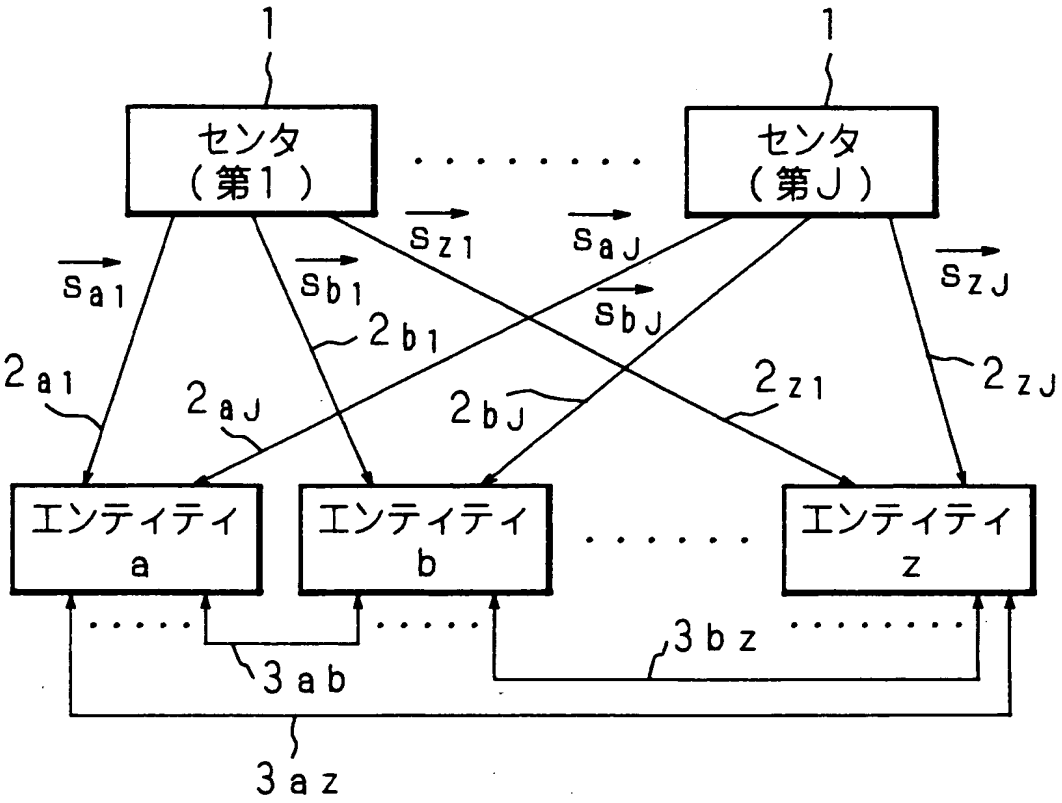
３０　通信路

４０　コンピュータ

４１，４２，４３　記録媒体

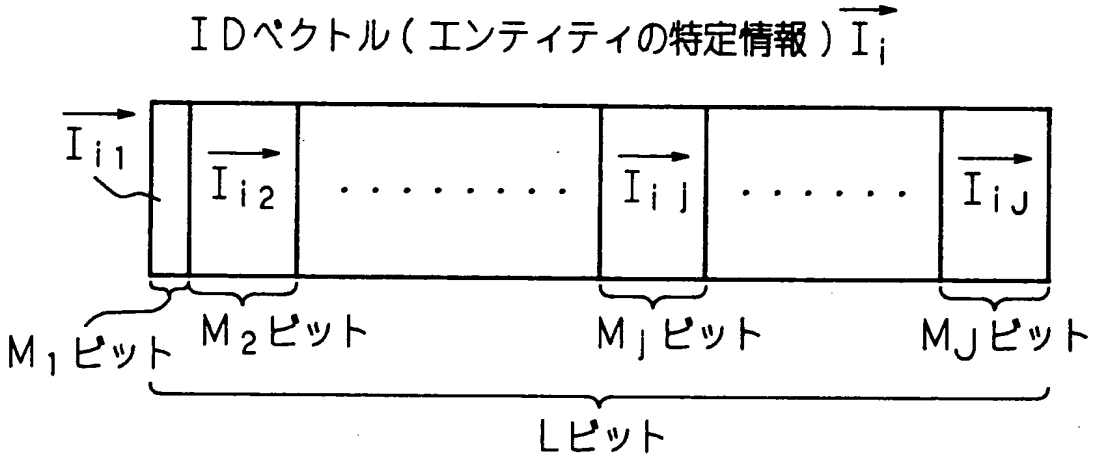
【書類名】　　図面

【図１】

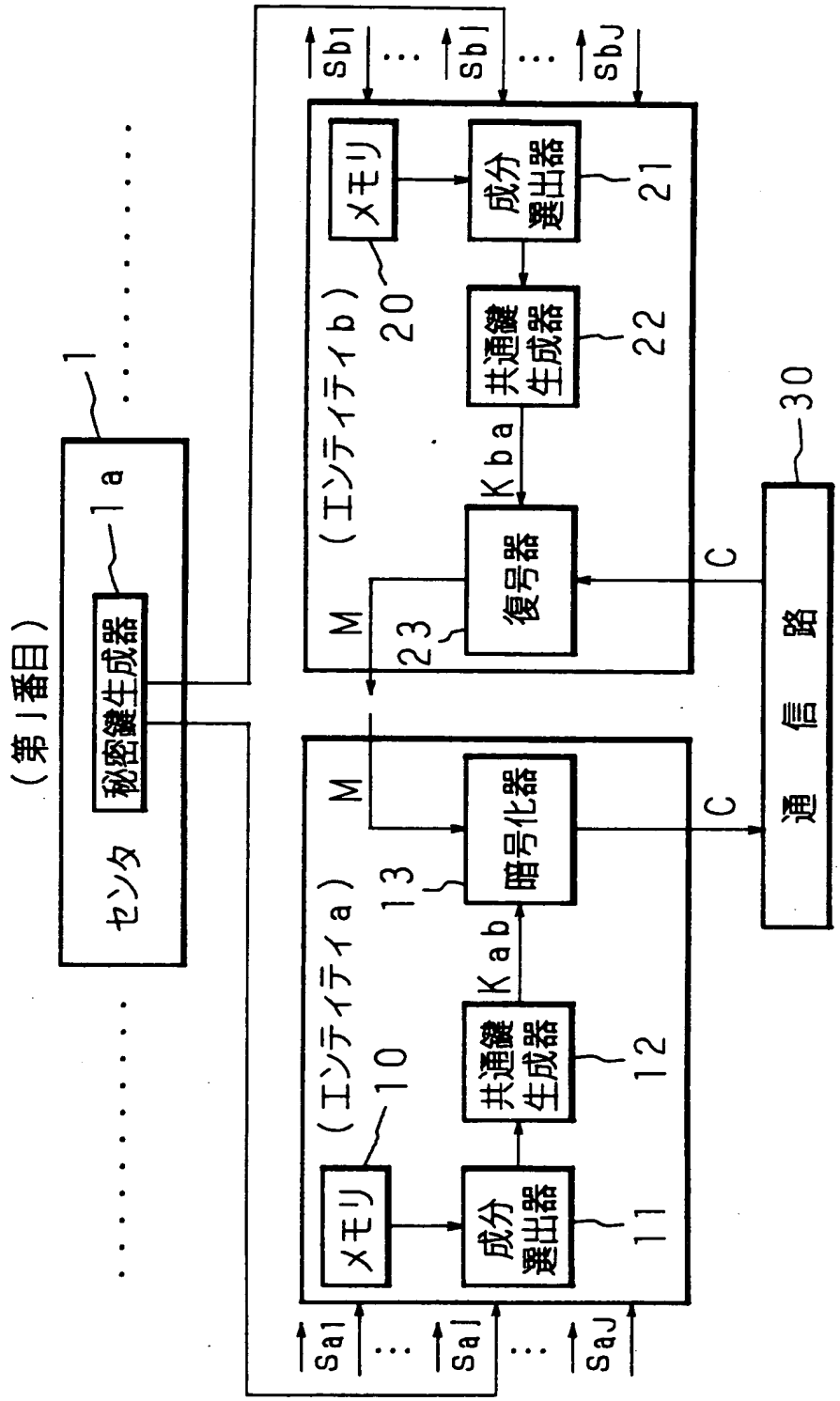


出証特２０００－３０６４８４２

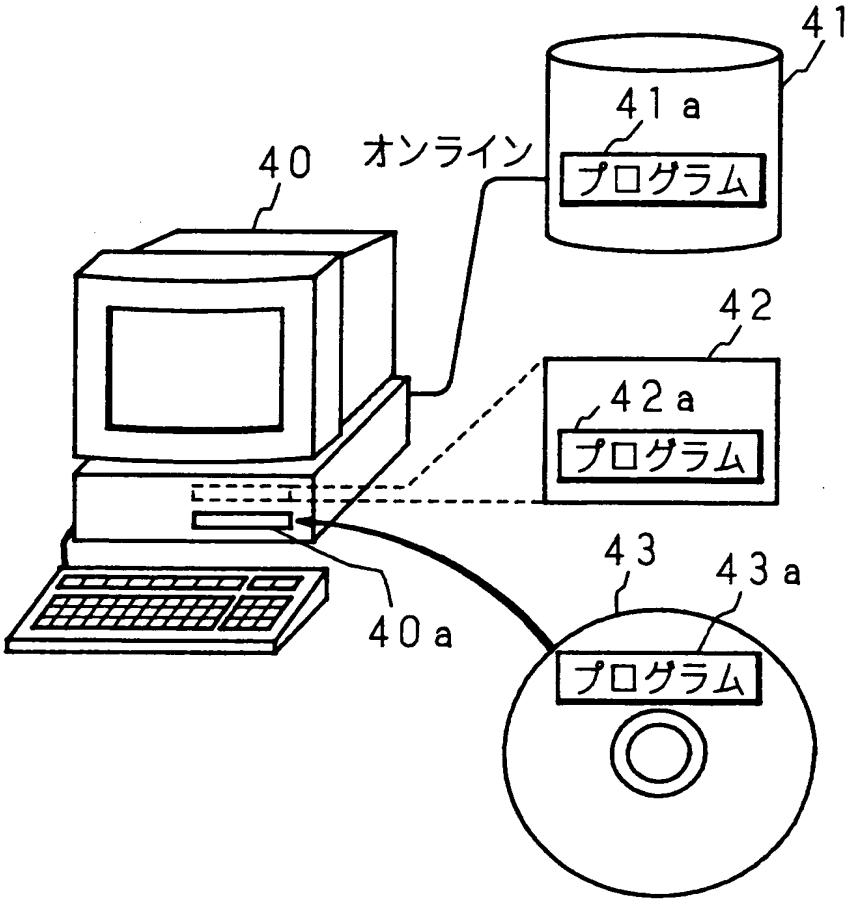
【図２】


ＩＤベクトル（エンティティの特定情報）$\vec{I_i}$
$\vec{I_{i1}}$
$\vec{I_{i2}}$
$\vec{I_{ij}}$
$\vec{I_{iJ}}$
M1ビット
M2ビット
MJビット
Mjビット
Lビット

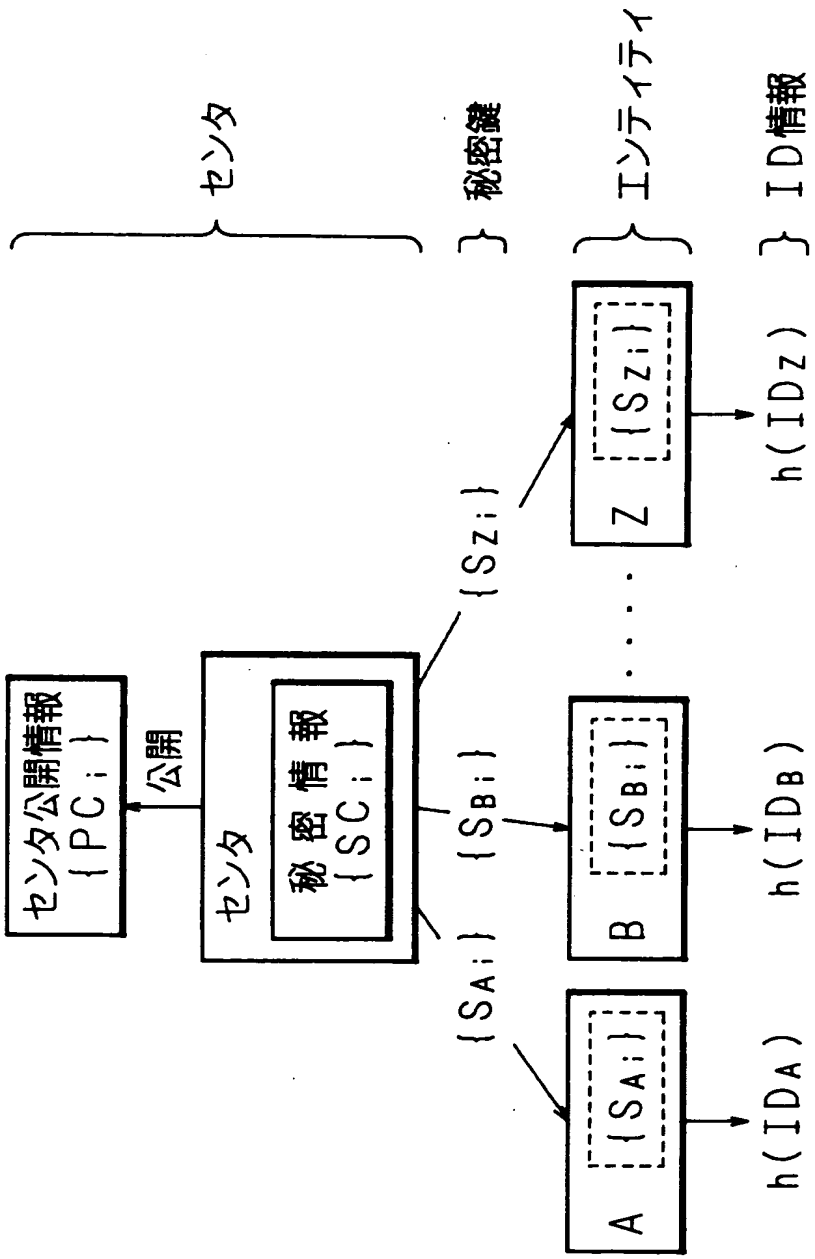
【図３】


（第１番目）
センタ
秘密鍵生成器
1a
1
Sa1
Sal
SaJ
（エンティティａ）
メモリ
10
成分選出器
11
共通鍵生成器
12
Kab
暗号化器
13
M
C
通信路
30
（エンティティｂ）
メモリ
20
成分選出器
21
共通鍵生成器
22
Kba
復号器
23
M
C
Sb1
Sbl
SbJ

【図４】



【図５】


センタ
秘密鍵
エンティティ
ID情報
センタ公開情報
{PCi}
公開
センタ
秘密情報
{SCi}
{SZi}
{SBi}
{SAi}
Z
{SZi}
B
{SBi}
A
{SAi}
h(IDZ)
h(IDB)
h(IDA)

【書類名】　　要約書

【要約】

【課題】　ＩＤ－ＮＩＫＳ暗号通信システムにあって、安全性を向上しながら新規のセンタを容易に追加できる秘密鍵生成方法，暗号化方法及び暗号通信方法を提供することを目的とする。

【解決手段】　各センタ１にて、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成する。所定の複数ビット列からなる原ハッシュ値列から各センタ１毎に複数の任意の番目のビットを選択して各センタ１毎のハッシュ値を設定する。新規のセンタ１を既存の複数のセンタ１に追加した際に、既存の複数のセンタ１に設定されているハッシュ値を並べた原ハッシュ値列から任意の番目のものを選択することにより、既存の複数のセンタ１のハッシュ値を変えないで、新規のセンタ１のハッシュ値を設定する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－０１６３５８
受付番号	５００００７３７３７
書類名	特許願
担当官	塩崎　博子　　１６０６
作成日	平成１２年　７月１２日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000006297
- 【住所又は居所】 京都府京都市南区吉祥院南落合町３番地
- 【氏名又は名称】 村田機械株式会社

【特許出願人】
- 【識別番号】 597008636
- 【住所又は居所】 大阪府箕面市粟生外院４丁目１５番３号
- 【氏名又は名称】 笠原　正雄

【復代理人】
- 【識別番号】 100114557
- 【住所又は居所】 大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所
- 【氏名又は名称】 河野　英仁

【代理人】 申請人
- 【識別番号】 100078868
- 【住所又は居所】 大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所
- 【氏名又は名称】 河野　登夫

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　大阪府箕面市粟生外院４丁目１５番３号
氏　名　笠原　正雄